نظرة على قدرات "اسرائيل" في الحرب الالكترونية

Think Tanks Monitor2016-03-28

اختراق ممنهج لاميركا

استيقظ الاميركيون صبيحة يوم 23 من الشهر الجاري على خبر فريد شديد الاقتضاب، نقلته شبكة بي بي سي البريطانية، وغير مسبوق يفيد بتراجع مكتب التحقيقات الفيدرالي، ووزارة العدل الاميركية، عن دعواهما القضائية ضد شركة "آبل" العملاقة، بعد مقاومتها تيسير دخول الاجهزة الأمنية الرسمية لبرامجها الخاصة بالهواتف الذكية.

الشق الاول في الخبر: "صباح يوم الاثنين، 21 آذار الجاري، ارجأ مكتب التحقيقات الفيدرالي (اف بي آي) متابعته القضية القانونية المرفوعة قائلا ربما تمكن "طرف ثالث غير حكومي" من التوصل لطريقة تخترق جهاز الهاتف دون الحاجة لمساعدة شركة آبل."

ونقلت الشبكة عن مكتب الأف بي آي قوله "يتعين علينا اختبار تلك الطريقة.. ولهذا تقدمنا من المحكمة بتوسل لاتاحة فرصة زمنية اطول لطَرْق هذا الخيار." واضافت ان "الطرف الثالث عرض تجربته يوم الاحد، 20 آذار.. وعلينا الانتظار."

الشق الثاني والاهم: "شركة اسرائيلية للهواتف النقالة (سيليبرايت) توفر الدعم لمكتب التحقيقات الفيدرالي لفك شيفرة جهاز الهاتف العائد لسيد رضوان فاروق، الذي أطلق النار برفقة زوجته على موظفين مدنيين في سان بيرنادينو كاليفورنيا." وعليه، لن تحتاج وزارة العدل واجهزتها الاخرى تعاون شركة "آبل" لاختراق شيفرة الجهاز المذكور "في حال نجاح شركة سيليبرايت."

واضافت شبكة (بي بي سي) ان شركة "سيليبرايت ابرمت عقدا مع الأف بي آي عام 2013 لتحليل قضايا حاسوبية.. وعقدا جديدا أخرا عقب رفض شركة آبل الامتثال لطلب الجهاز العمل على برنامج خاص لنظام تشغيلها من شأنه اعاقة جهود الغاء محتويات الجهاز ان تعرض لمحاولات متتالية

لاستخراج كلمة السر."

واردفت ان "سليبرايت وفرت خدمات مماثلة لأجهزة الأمن البريطانية، مما اتاح لها القاء القبض على شخص مطلوب عام 2012 بعد استرجاع الرسائل النصية الملغاة من جهاز آي فون."

هوية تجارية بأهداف عسكرية

تأسست شركة "سيليبرايت" عام 1999 في فلسطين المحتلة، ومقرها مستعمرة "بتاح تكفا" القريبة من مدينة يافا، لتطوير جهاز لاستخراج البيانات المخزنة على اجهزة اتصال محمولة، من بينها الهواتف النقالة والاجهزة اللوحية، والتوصل لاستعادة البيانات الملغاة من قبل المستخدم، وفك التشفير وكلمات السر. ولدى الشركة مكاتب فرعية في ولاية نيوجيرسي والمانيا ايضا، يصل طاقمها التقني الى نحو 500 فرد.

تزعم الشركة ان قدراتها تتمثل في استغلال الذاكرة السريعة المتضمنة في كافة الهواتف النقالة، والتي تستند الى بيانات لوغاريتماتية ترمي لتخزين بيانات الهاتف لاطول فترة ممكنة، حتى بعد اقدام المستخدم على الغائها.

لا تخفي "الشركة" علاقاتها الوثيقة "والعميقة بالجيش واجهزة الاستخبارات الاسرائيلية،" وخاصة "وحدة 8200 للتجسس الالكتروني" التي تعد المصدر البشري للشركة؛ وتضم بين رؤسائها ضباط سابقون، منهم عميت غروس مدير ابحاث الاجهزة النقالة، وشاحار طال المدير العام السابق للوسائل التقنية في الجيش. وما رشح عن نشاطاتها الاستخباراتية اقرارها بامتلاك القدرة على فك رموز الرسائل النصية المرسلة عبر تطبيق "تلغرام،" الذي قيل ان نشطاء الدولة الاسلامية يستخدمونه بكثرة.

اختراق الشركة للأجهزة الاميركية نمى الى مسامع النقابة الاميركية للحقوق المدنية، عام 2011، من قبل فرعها في ولاية ميتشيغان الذي سعى للحصول على اجوبة من جهاز الشرطة المركزي في الولاية حول استخدام عناصره "معدات تصنعها سيليبرايت لتنفيذ مهام غير قانونية بتفتيش اجهزة

الهواتف النقالة للمواطنين."

في عام 2013 اصدر مكتب التحقيقات الفيدرالي مذكرة داخلية يعلن فيها عن نيته "شراء اجهزة تصنعها سيليبرايت.. وهي احدى القلائل التي تملك القدرة على استعادة سريعة للصور واشرطة الفيديو، وسجل البيانات الملغاة والرسائل النصية بدقة تصل نحو 59% لكافة اجهزة الهواتف النقالة – تتضمن عدة نماذج من اجهزة آي فون."

سعت الحكومة الاميركية لتخفيف الانتقادات المتوقعة، حول نفوذ شركة "اجنبية" تمنحها صلاحية اختراق البيانات الخاصة، بإعادة تركيز الانظار على "الخطر الايراني" في مجال الحرب الالكترونية، ووجهت تهما لسبعة افراد "مدعومين من ايران حاولوا تعطيل عمل سد للمياه في ولاية نيويورك.. واختراق اجهزة الكمبيوتر الخاصة ببورصة نيويورك ومؤسسات مصرفية اخرى لنحو 40 شركة اميركية." الافراد المتهمون لا يزالوا طلقاء ويجري البحث عن اماكن اقامتهم.

في الوقت عينه، وبالتزامن مع توجيه التهم القضائية، اعدت وزارة المالية الاميركية لائحة بإجراءات مقاطعة ضد عدة اشخاص ايرانيين على خلفية اطلاق طهران تجارب على صواريخ باليستية، وصفتها يومية واشنطن تايمز اليمينية، 24 آذار، بانها أتت لتعزيز عزم ادارة الرئيس اوباما عدم الرضوخ لإيران امام خصومه السياسيين.

واضافت الصحيفة ان لائحة الاتهام للسبعة تعد "المرة الاولى التي تلجأ اليها الاجهزة الحكومية ملاحقة مواطنين (اميركيين) متهمون بالتعامل مع دولة اجنبية بهدف عرقلة اداء اجهزة البنية التحيتة في الولايات المتحدة."

اوضحت نائبة رئيس لجنة الاستخبارات في مجلس الشيوخ، دايان فاينستاين، عمق القلق في الدوائر الرسمية بالقول "ان استطاع القراصنة الظفر بالسدود، وشبكة توزيع الكهرباء، والمطارات، ومصادر المياه او المفاعلات النووية، فان حجم الضرر الناجم عنها سيكون هائلا."

البعد السعودي

لسنا هنا بصدد الاشارة الى تنامي العلاقات "الرسمية" بين الرياض وتل ابيب، اذ انها ليست بحاجة لتقديم الدلائل والقرائن سيما وان اصحابها لا يخجلون من الاعراب عن تلازم علاقتهم ومصيرهم السياسي بالكيان الصهيوني.

الامر الاهم هو الذي يتعلق بالحرب الالكترونية، التي تفتقد السعودية لأي من مكوناتها ومستلزماتها التقنية والبشرية، بينما يقتصر دورها التمويلي تكملة لوظيفتها في خدمة الاستراتيجية الاميركية، واستراتيجية الكيان الصهيوني دون مساحيق تجميلية.

هنا المسألة تتعلق بتضافر الجهود الاميركية "والاسرائيلية" في استهداف اجهزة الطرد المركزية في ايران، ببرامج الكترونية ضارة، اشهرها "ستاكسنت و فلايم."

المؤرخ الاميركي البارز باري لاندو، صاحب كتاب "شبكة من التضليل: تاريخ التواطؤ الغربي في العراق، منذ شرشل لكندي وجورج دبليو بوش،" ينقل عن تقرير صادر عن "جامعة تل ابيب" مطلع العام الجاري يشير فيه الى السعودية بأنها "الأمل الاخير وخط الدفاع عن اسرائيل.. فالسعوديون يشكلون الأمل النهائي للدولة اليهودية لحماية مصالحها السياسية في العالم العربي."

ويضيف نقلا عن "مصدر خاص رفيع في الحكومة الاسرائيلية" قوله ان "رئيس الموساد الاسرائيلي قصد السعودية عدة مرات للبحث مع نظرائه هناك (تركي الفيصل ولاحقا بندر بن سلطان) ابرام اتفاقية من شأنها تُقدم السعودية على تمويل جهود (اسرائيل) تنفيذ جملة اغتيالات لعدد من كبار علماء الذرة في ايران.. تتقاضى بموجبها مليار دولار." واستطرد بالقول ان مصدره الرفيع قال ان السعوديين "اعتبروا المبلغ رخيصا مقابل حجم الضرر الذي سيلحق ببرنامج ايران النووي."

ليس من العسير الذهاب بالقول ان ما يتيسر من امكانيات تقنية لدى "سيليبرايت" سيسخّر (او انه مسخّر عمليا) في خدمة الحكومة السعودية مقابل اموالا طائلة ايضا؛ بل لدول الخليج الاخرى ان لم تكن مجتمعة فباغلبيتها.

القرصنة صناعة ومهنة

في لحظة نادرة من الصراحة العلنية، اوضح رئيس جهاز الاستخبارات العسكرية "الاسرائيلية،" عاموس يادلين، طموحات وخطط جهازه لتسخير التقدم التقني والالكتروني في برامج عسكرية. وقال في نهاية عام 2009 امام "معهد دراسات الأمن الوطني،" احد نخب مراكز الابحاث الصهيونية، "دعوني اوضح لكم امام هذا المنبر المرموق ان مجال الحرب الالكترونية يتطابق تماما مع العقيدة الدفاعية لدولة اسرائيل.. وهو مجال لا نستطيع فيه الاعتماد على دعم خارجي او تقنية ليست من صنعنا."

تشير البيانات الاقتصادية المتوفرة الى قطاع مزدهر في مجال التقنيات الالكترونية "الاسرائيلية،" بلغت وارداتها عام 2015 وحده نحو 6 مليارات دولار، استقطبت نحو 20% من اليد العاملة في قطاع الاستثمارات الخاصة؛ فضلا عن عائدات التصدير التي تفوق احيانا صادرات "الاسلحة الاسرائيلية."

جذور برنامج الأمن الالكتروني، بكافة تلاوينه وتطبيقاته، تجد ارضيتها في قطاع المؤسسة العسكرية "الاسرائيلية،" كأكبر وأضخم جهاز في الكيان يعززها الاستثمارات المستدامة والعالية في المجالات العسكرية المختلفة، لا سيما في قطاع الاستخبارات. من المعلوم ايضا ان عددا لا بأس به ممن خدم في تلك الاجهزة استفاد من خبرته التقنية لتوظيفها في اعمال "تجارية" الطابع لخدمة اهداف واحتياجات المؤسسة العسكرية. كما ان السياسة "الحكومية تنحاز لتقديم مختلف التسهيلات والاعفاءات الضريبية."

للإضاءة على نمط العلاقة التبادلية علينا الاشارة الى ابرز برامج "الأمن الالكتروني" الخاص بالشبكات، برنامج "شيك بوينت،" الذي اضحى البرنامج المفضل للحضور الالكتروني الاميركي منذ عقد التسعينيات. يترأس شركة "شيك بوينت" غيل شويد، بعد خروجه من الخدمة الفعلية لاهم الوحدات الالكترونية "السرية – وحدة 8200" في المؤسسة العسكرية "الاسرائيلية" حقق فيها منصبا "رفيعا بالغ السرية." ويستقطب شويد موظفيه من صفوف الاجهزة العسكرية والالكترونية، احدهم الرئيس السابق لتلك الوحدة، نير ليمبيرت، وآخرين.

في مطلع العام الجاري عقد مؤتمر في تل ابيب "سايبرتك 2016" استقطب الاف الكفاءات التقنية من الخارج، بحضور بنيامين نتنياهو، كان احد محاوره "الأمن الالكتروني للسيارات." يذكر ان تقنية

الالكترونيات الحديثة تدخل في مكونات صناعة السيارات مما يجعلها عرضة للقرصنة والتسبب في تعطيل الكوابح عن بعد وربما مقتل ركابها.

جاءت اشارة عابرة لاهتمام "اسرائيل" بتقنية الكترونيات السيارات في مقال نشر عام 2014 اوضح ان "القيادات العليا تولي اهتماما عاليا لتلك المسألة منذ عدة سنوات" تتعلق بتطبيقات مختلفة لقرصنة الاجهزة السيارة، بل ان "بعض المنظمات ودول اخرى باستطاعتها الحاق الضرر بأهداف وشخصيات محددة عبر شبكة الانترنت."

واستفاض مصدر المقال بالاشارة "الافتراضية" لرغبة جهاز استخباراتي معين التخلص من شخصية ما في بلد اجنبي "عبر السيطرة على اجهزة التحكم الالكترونية في سيارة يقودها، عادة ما تكون حديثة العهد. حينئذ ما عليك الا اجراء اتصال عن بعد مع اجهزة الكمبيوتر بداخل السيارة، ومعرفة كيفية تتبع اي جهاز محمول في حوزة السائق، حتى لو كان خارج الخدمة او معطلا. باستطاعتك حينها متى ستحاول السيارة السير في منحدر منخفض والتحكم بإبطال عمل نظام الكوابح حالا. عندئذ تكون قد حكمت على نهاية كل من كان بداخل السيارة."

من نافل القول ان اعضاء تلك المؤسسة الالكترونية يستغلون ميزاتهم الاقتصادية الى ابعد حد، للانخراط في صفقات "تجارية" مع نظم متعددة لا سيما في دول العالم النامي في منطقة آسيا الوسطى بشكل خاص، جورجيا واذربيجان مثالا، بما يمكنها من الحصول على بيانات حصرية غير مقيدة لمعلومات تخص اتصالات مواطني تلك الدول ونشاطاتها المتعددة على شبكة الانترنت، دون رقيب.

يشار الى ان "بعض تلك الشركات الاسرائيلية" وجهت لها تهم مساعدة جهود وكالة الأمن الوطني الاميركية في التلصص والتجسس على المواطنين الاميركيين.

هيكلية اجهزة الحرب الالكترونية

بالإشارة الى "وحدة 8200" عالية السرية فإنها تتخذ مقرا لها في صحراء النقب، وتطورت تدريجيا من

جهاز اشارة ملحق بالجيش "الاسرائيلي" الى أبرز الاجهزة في مجال الحرب والقرصنة الالكترونية. احدى الشركات الاميركية المختصة بتقييم صلاحية الشركات والمنشآت الاخرى اعتبرت "وحدة 820 من بين مجموعة من ستة لكبار الاجهزة المبادرة للهجمات الالكترونية في العالم."

من ضمن اولويات الوحدة المذكورة ما يعرف "بجرف المعلومات والبيانات، والتعامل مع كم هائل منها يقدر بالملايين للتوصل الى معلومة تعتبرها مهمة، والتعرف على عادة التكرار في البيانات مما يؤشر على مسار غير سوي ضمن تصنيفاتها."

تشتهر تلك الوحدة ايضا بقدرتها على انتاج البرامج الضارة – الفايروسات. وقد اوضح المتعاقد السابق مع وكالة الأمن الوطني، ادوارد سنودن، لمجلة دير شبيغل الالمانية ان "اسرائيل ساعدت الولايات المتحدة في انتاج فايروس ستاكسنت.. عام 2010" ضد اجهزة الطرد المركزية في ايران.

جهود "وحدة 8200" للتجسس وتجنيد الفلسطينيين لا تعرف حدودا لها، ولا تقتصر على العناصر المصنفة "معادية لاسرائيل" فحسب، بل لافراد عائلاتهم واقربائهم وجيرانهم، وكل من قد يشكل مصدرا للمعلومات تخص "الحالة الصحية والوضع المالي والمسلك الشخصي" للفرد.

رئيس الاركان غادي ايزنكوت كافأ "وحدة 8200" بتطوير وضعها الميداني الى "قيادة سايبيرية،" بقرار اصدره مطلع الصيف الماضي،، يخولها بموجبه "الاشراف على كافة الانشطة العملياتية في الفضاء الافتراضي." ونجح بعض المنتسبين اليها باجتياز دورة تدريبية في نهاية العام الماضي، امتدت اربعة اشهر.

وفق تلك الرؤيا، من المتوقع ايلاء "القيادة السايبيرية" مهاما هجومية ودفاعية في آن، بتنسيق وثيق مع الوحدات الميدانية الاخرى لاختراق اجهزة التحكم والسيطرة للطرف المعادي.

* نشرة التقرير الأسبوعي لمراكز الابحاث الأميركية

.....

* الآراء الواردة لا تعبر بالضرورة عن رأي شبكة النبأ المعلوماتية